UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

CHRISTOPHER HARLAN and SARA HARLAN, Plaintiffs, v. CROWDSTRIKE HOLDINGS, INC., and CROWDSTRIKE, INC., Defendants	Civil Action No. <u>1:24-cv-00954</u> **CLASS ACTION** **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

I.   INTRODUCTION

1.   Many large businesses, like major airlines, and government agencies use software from CrowdStrike Holdings, Inc. and CrowdStrike, Inc. (collectively, "CrowdStrike"), one of the largest cybersecurity companies, to keep their many computer terminals secure from hackers. CrowdStrike attaches deeply within the Windows operating system to anticipate innovative hackers, but that deep-level attachment also gives CrowdStrike greater ability to trigger a computer failure.[1]

2.   CrowdStrike's executives knew their design involved the operating system and knew its many airline customers would have difficulty repairing numerous blue failure screens on

---

[1] Joseph Menn and Aaron Gregg, *CrowdStrike Blames Global IT Outage on Bug in Checking Updates,* THE WASHINGTON POST (July 24, 2024), https://www.washingtonpost.com/business/2024/07/24/crowdstrike-microsoft-crash-bug-report/ (accessed July 31, 2024)

all their terminals and kiosks.[2]   CrowdStrike's CEO told investors its many airline customers

"don't want to send out an IT person to go fix a kiosk that has a Microsoft blue screen," so the

airlines should exclusively use CrowdStrike's Falcon security platform.[3]   CrowdStrike also knew

that it pushed updates out nearly simultaneously to all of its customers and all of their computer

networks, which, as its prior experiences showed, could crash computers that would get stuck

trying repetitively but unsuccessfully to reboot.

3.   Despite that knowledge, early on Friday, July 29, 2024, CrowdStrike pushed out an

ill-designed and poorly tested update to its Falcon software, causing the largest computer outage

in history (the "CrowdStrike Outage").   Delta Airlines especially relied on CrowdStrike for its

many Windows computers and terminals.

4.   As a result of the Outage, thousands of Delta's computers crashed and had to be

manually rebooted.   Delta could not even locate many of its flight crews because that information

was in the computers.   As a direct result of CrowdStrike's knowing negligence, Delta had to cancel

thousands of flights, stranding, and confounding the travel of, thousands of travelers that Delta had

promised to deliver on time to their destinations, destroying the value of many events for which

customers had paid, and collectively costing these travelers millions of dollars.   But for the failures

---

[2] The "blue screen of death" appears on Windows computer screens when a critical error (or "stop error") has caused the Windows operating system to crash, often indicating an error in the operating system's deeper levels.   Davey Winder, *Blue Screen of Death—Microsoft Says Turn It Off And On Again And Again And Again*, FORBES (July 20, 2024), https://www.forbes.com/sites/daveywinder/2024/07/20/blue-screen-of-death-microsoft-says-turn-it-off-and-on-again-and-again-and-again/ (accessed August 9, 2024).

[3] *See CrowdStrike Holdings, Inc. (CRWD) Q3 2024 Earnings Call Transcript*, SEEKINGALPHA (Nov. 28, 2023), https://seekingalpha.com/article/4654747-crowdstrike-holdings-inc-crwd-q3-2024-earnings-call-transcript (accessed August 1, 2024).

and harms caused by CrowdStrike, which were foreseeable, Plaintiffs and Class Members would not have been damaged.

5.   Accordingly, Plaintiffs bring this action to redress the CrowdStrike's knowing and careless disruption of Delta's systems and its promises to its travelers.

II.   JURISDICTION AND VENUE

6.   This Court has subject matter jurisdiction under the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. §§ 1332(d)(2) and (6) because (i) there are 100 or more class members, (ii) the aggregate amount in controversy exceeds $5,000,000 exclusive of interest and costs, and (iii) the case has minimal diversity because at least one plaintiff and one defendant are citizens of different states.

7.   Venue is also proper in this judicial district under 28 U.S.C. § 1391 because Defendant transacts substantial business here. On information and belief, CrowdStrike supplied software to Delta for computer equipment operating in this district and therefore received revenue and profits from its subscriptions in this district. The Austin, Texas, airport was among the airports where the CrowdStrike Outage affected Delta flights.[4]

8.   This Court has personal jurisdiction over CrowdStrike by virtue of its transactions, business presence, and business conducted in this judicial district. Defendant CrowdStrike has transacted and done business and committed knowing negligence and interfered with contracts in

---

[4] Rachel Royster, *Austin Air Travel Affected by CrowdStrike Outage; CapMetro Public Transit Back on Track*, AUSTIN-AMERICAN STATESMAN (July 19, 2024), https://www.statesman.com/story/news/local/2024/07/19/austin-bergstrom-international-airport-cancel-travel-crowdstrike-tech-outage-capmetro-public-transit/74470631007/ (accessed August 9, 2024).

this judicial district by pushing its defective software update to computers in this State and violated common law negligence doctrine in this State and district.

III.   PARTIES

9.   Plaintiff Christopher Harlan is a citizen of Iowa and resides in Urbandale, Iowa.

10.   Plaintiff Sara Harlan is a citizen of Iowa and resides in Urbandale, Iowa. Sara Harlan and Christopher Harlan are married and are sometimes referred to collectively as "Plaintiffs."

11.   Plaintiffs purchased airline tickets for to return from their vacation in the Dominican Republic to Atlanta, Georgia, and then to fly on Delta from Atlanta home to the Des Moines, Iowa, airport on July 22, 2024. As a result of the CrowdStrike Outage, Delta canceled Plaintiffs' flight from Atlanta to get home.

12.   Plaintiffs each spent time booking replacement flights home, only to find replacement flights were canceled, sometimes after multiple delays. One flight was from Atlanta to Omaha, Nebraska, so Plaintiff Christopher Harlan booked a rental car to drive from Omaha to Des Moines. The flight to Omaha was also delayed and then canceled.

13.   Plaintiff Sara Harlan booked a hotel room in Atlanta for the rest of the night of July 22, 2024, using their joint credit card. Plaintiffs took an Uber ride to the hotel, leaving the airport after midnight. At the hotel, they had to wait an hour to check in, finally getting to their room around 2:30 a.m. Their hotel room cost $139.60. They also incurred an Uber ride back to the airport. Their Uber rides to and from the airport cost $35.04.

14.   Plaintiffs finally boarded a flight that traveled on July 23, 2024, and they arrived in Des Moines on that date. In Iowa, Plaintiffs paid for extra parking at the airport and for an extra day of house-sitting.

15.   As a result of the CrowdStrike Outage and Plaintiffs' delayed flights, they incurred out-of-pocket expenses that would not otherwise have been required. His additional expenses included food at the airport on July 22 and 23, 2024, a night at the hotel, Uber rides to and from the hotel, and additional parking and house-sitting.

16.   CrowdStrike Holdings, Inc., is incorporated in Delaware. CrowdStrike started in Sunnyvale, California, in Silicon Valley, but designated Austin, Texas, as its headquarters in 2021. CrowdStrike Holdings controls its subsidiaries and conducts its business through subsidiaries acting as its agents, including CrowdStrike, Inc.

17.   CrowdStrike, Inc., is a Delaware corporation with its principal place of business in Austin, Texas. CrowdStrike, Inc. is a direct subsidiary of CrowdStrike Holdings, Inc. CrowdStrike Holdings, Inc., and CrowdStrike, Inc., are collectively referred to as "CrowdStrike." CrowdStrike considers its accounting on a consolidated basis and considers itself as one operating and reportable segment.

18.   CrowdStrike is a cybersecurity enterprise. CrowdStrike's primary offering is its Falcon platform. CrowdStrike has over 8,400 employees, collected over $23 billion in 2023 revenue, and serves about 29,000 customers, including many Fortune 500 airlines and other companies.

IV.   FACTUAL ALLEGATIONS

19.   With a $77.4 billion 2024 market valuation, CrowdStrike is the second-largest global cybersecurity company. Palo Alto Networks has the largest market capitalization. Other large cybersecurity companies include Fortinet, Cloudflare, Zscaler, Check Point Software,

Leidos, Okta, Akami, and Gen Digital.[5] Corporate business antivirus tools differ from consumer antivirus products in that business tools protect a network of devices within an organization. Business security tools are referred to as endpoint security "because they protect multiple devices under a single network, and these devices are called endpoints."[6]

A.   CrowdStrike Falcon and Endpoint Security Protection Software.

20.   Consumer antivirus products tend to be reactive and focus on preventing known malware from infecting that device. Each device requires a separate software installation. Consumer antivirus software scans devices for signatures associated with malware and compares them to databases of known malware signatures that the antivirus companies maintain.[7]

21.   Business endpoint cyber-security software is more proactive in preventing attacks from occurring. Those programs "usually employ artificial intelligence and machine learning to detect threats whose signatures may not be known." The artificial intelligence may be used to "identify threat patterns and stop them before they can cause issues."[8]

22.   Revenue for the global endpoint security market is forecast to grow from $16.25 billion in 2024 to $36.59 billion in 2028.[9]

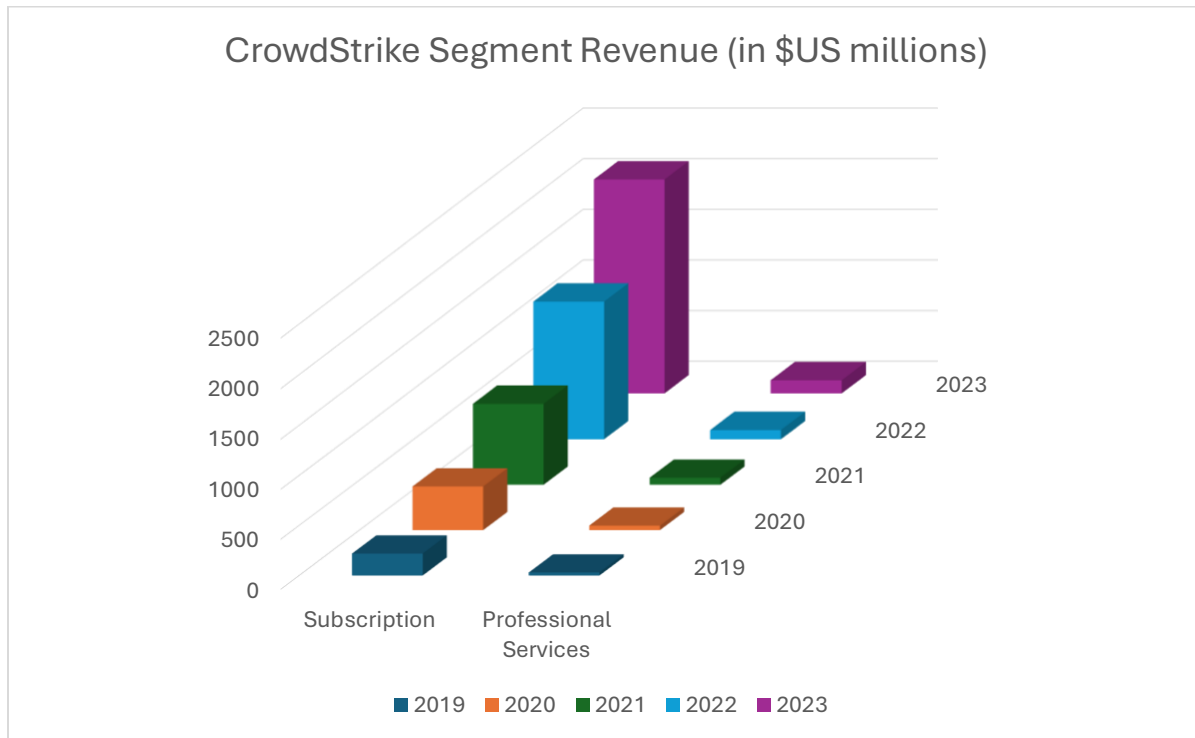[5] Statista Report, COMPANIES & PRODUCTS—CROWDSTRIKE at 7 (2024).

[6] Benedict Collins, *Best Endpoint Protection Software of 2024*, TECHRADAR PRO (June 26, 2024), https://www.techradar.com/news/best-endpoint-security-software (accessed August 1, 2024).

[7] *Id.*

[8] *Id.*

[9] *Forecast Revenue from Endpoint Security Market Worldwide Form 2024 to 2028*, STATISTA (2024), https://www.statista.com/statistics/497965/endpoint-security-market/ (accessed August 1, 2024).

23.   CrowdStrike's cyber-security solutions include endpoint protection, threat intelligence, incident response, and endpoint detection and response.[10] CrowdStrike's customers include government agencies and multinational corporations in several industries including airlines, banks, hospitals, and telecommunications firms.[11] CrowdStrike's subscription revenue grew from $219.4 million in 2019 to $2.11 billion in 2023, considerably surpassing its professional services revenue.[12] Accordingly, CrowdStrike knew most of its work was for ongoing customers such as Delta Airlines.

CrowdStrike Segment Revenue (in $US millions)

---

24.   CrowdStrike's flagship service is its Falcon software platform, which is said to use machine learning and other artificial intelligence to detect, prevent, and respond to cyber-security threats. CrowdStrike claims Falcon's key advantage is its ability to keep up with threats through rapid innovation. CrowdStrike claims its platform collects data to identify hackers' shifting tactics and continuously improves to keep customers ahead of attackers' newest approaches.

25.   CrowdStrike's Falcon software, like other security platforms, attaches to Microsoft Windows deeply within the Windows operating system.[13] CrowdStrike regularly updates the platform in at least two ways. First, "Sensor Content" updates directly affect Falcon's sensor. Second, "Rapid Response Content" updates adjust how those sensors behave in trying to detect threats.

B.   The Global CrowdStrike Outage.

26.   Shortly after midnight Eastern time on the morning of July 19, 2024, CrowdStrike pushed out a defective update for its Falcon platform. CrowdStrike intended the update to provide what it calls Rapid Response Content to its sensor malware detection component.

27.   Because Falcon is an endpoint system, CrowdStrike pushed the update simultaneously to thousands of separate computer endpoints—likely to most computer terminals in Delta's computer network, as well as to each endpoint in thousands of other computer networks that CrowdStrike services.

28.   CrowdStrike included a defective data file in the update it sent to the detection unit's Content Interpreter. The defect caused an out-of-bounds exception in the Windows software.

---

[13] Menn and Gregg, *supra*.

At Windows' deeper level of the operating system, crashes can more readily spread across the operating system than at the more surface level at which user's visible programs normally operate.

29.   CrowdStrike's defect and its out-of-bounds exception caused many of these computer endpoints to crash.

30.   CrowdStrike attempted to roll back its defective update at 1:27 a.m. Eastern time, but by then it had already affected millions of computers on numerous networks.[14]

31.   Because of the computer system crashes, users' computers greeted them with Windows' blue warning screen, often called the Blue Screen of Death.

32.   CrowdStrike's defective update further caused affected computers to shut down and endlessly, but unsuccessfully, attempt to reboot, sometimes called a "doom loop."

33.   The nature of these operating system crashes meant that each endpoint required manual intervention to restart.

34.   Accounts referred to the problems as "cascading instantly." A hospital operator's Chief Information Officer said 15,000 of its servers went down affecting 40,000 of its 150,000 computers.[15]

35.   CrowdStrike's defective Falcon update caused what has been described as the largest Information Technology (IT) outage in history, crashing millions of computers. Major

---

[14] Brian Fung, *We Finally Know What Caused the Global Tech Outage – and How Much it Cost*, CNN BUSINESS (July 24, 2024), https://www.cnn.com/2024/07/24/tech/crowdstrike-outage-cost-cause/index.html (accessed July 25, 2024).

[15] Adam Satariano, Paul Mozur, Kate Conger and Sheera Frenkel, *Chaos and Confusion: Tech Outage Causes Disruptions Worldwide*, NEW YORK TIMES (July 19, 2024), https://www.nytimes.com/2024/07/19/business/microsoft-outage-cause-azure-crowdstrike.html (accessed July 24, 2024) (including hospital system); Fung, *supra*; Tom Warren, *CrowdStrike Blames Test Software for Taking Down 8.5 Million Windows Machines*, THE VERGE (July 24, 2024), https://www.theverge.com/2024/7/24/24205020/crowdstrike-test-software-bug-windows-bsod-issue (accessed July 25, 2024).

airlines requested a "global ground stop" from the Federal Aviation Administration.[16] The outage

disrupted airlines, train networks, hospitals, and television stations.[17]

36.   A letter from two leaders of Congress' Homeland Security Committee, Mark Green

and Andrew Garbarino to CrowdStrike's CEO stated, "[i]n less than one day, we have seen major

impacts to key functions of the global economy, including aviation, healthcare, banking, media,

and emergency services."[18] Numerous Fortune 500 companies use CrowdStrike products. An

insurance firm estimated that the healthcare and banking industries were especially affected, with

Fortune 500 airlines next behind them. The outage may have cost Fortune 500 companies as much

as $5.4 billion, with Fortune 500 airlines losing a collective $860 million.[19]

C.   CrowdStrike's Outage Harmed Delta Airlines and Its Customers.

37.   Among the airlines, the CrowdStrike Outage hit Delta Airlines especially hard.

Delta canceled more than 5,000 flights between the start of the outage on early July 19, 2024, and

July 25, 2024, when Delta's flights reportedly resumed. The outage disabled Delta's crew-tracking

system, preventing it from locating pilots and flight attendants to reschedule flights. Even after

Delta got its systems running again, the crew tracking system remained dysfunctional and

overloaded.

---

[16] Letter from Congress Members Mark Green, M.D. and Andrew Garbarino to George Kurtz, CEO of CrowdStrike Holdings, Inc., Austin, TX (July 22, 2024).

[17] Eshe Nelson and Danielle Kaye, *What We Know About the Global Microsoft Outage*, NEW YORK TIMES (July 19, 2024), https://www.nytimes.com/2024/07/19/technology/microsoft-crowdstrike-outage-what-happened.html (accessed July 24, 2024).

[18] Letter from Congress Members Green and Garborino.

[19] Fung, *supra.*

38.   The CrowdStrike Outage shut down more than 37,000 Delta computers and affected over 1.3 million Delta customers.[20]

39.   Delta's Chief Information Officer said in a video to employees that Delta had to manually repair over 1,500 systems that had gone offline in a time-consuming restart process.[21]

40.   An early estimate stated CrowdStrike's Outage required Delta to manually restart 40,000 affected computer servers.[22] CrowdStrike referred Delta to CrowdStrike's remediation website, which instructed Delta to manually reboot every affected machine.[23] Delta's CEO Ed Bastian later said not all its servers came back "the way they left when they went off."[24]

41.   Bastian stated Delta especially relied on CrowdStrike, so it was difficult to decouple it from the Windows operating system. He stated, referring to CrowdStrike, "You can't come into a mission critical 24/7 operation and tell us we have a bug." He added the outage cost Delta half a billion dollars, including lost revenue and tens of millions of dollars a day for hotel costs and other customer compensation.[25] Delta's counsel stated Delta's backup systems also relied on CrowdStrike.[26]

---

[20] Letter from David Boies to Michael Carlinsky at 1 (Aug. 8, 2024).

[21] Gareth Vipers and James Rundle, *CrowdStrike Explains What Went Wrong Days After Global Tech Outage,* WALL ST. J. (July 24, 2024), https://www.wsj.com/articles/crowdstrike-software-bug-global-tech-outage-96a9c937?mod=tech_lead_pos3 (accessed July 25, 2024).

[22] Roberto Torres, ed., *Delta Grapples with $500M in CrowdStrike Outage Costs*, CIO DIVE, (July 31, 2024), https://www.ciodive.com/news/delta-crowdstrike-outage-costs/722970/ (accessed July 31, 2024). Similarly, United Airlines manually rebooted over 26,000 computers. *Id.*

[23] Letter from David Boies to Michael Carlinsky at 2.

[24] Kelly Yamanouchi, *Delta CEO: CrowdStrike Outage Cost Airline 'Half a Billion Dollars*, THE ATLANTA-JOURNAL CONSTITUTION (July 31, 2024).

[25] *Id.*

[26] Letter from David Boies to Michael Carlinsky at 3.

42.   Delta's customers continued to suffer the effects of the outage for days after other airlines resumed normal operations. An estimated half a million customers were left waiting for hours in crowded airports while flights were repeatedly delayed only to be eventually canceled.[27] Customers unable to access Delta's website spent hours in line or on the phone to be booked on other flights that were also canceled. Others resorted to booking on other airlines or renting cars, frequently without luggage that arrived at their destination without them.[28]

43.   Delta's efforts to compensate customers only cover a portion of the costs incurred as a direct result of the CrowdStrike Outage. Delta's offer to reimburse out-of-pocket expenses such as hotel rooms, meals, and ground transportation is limited to largely undefined "reasonable costs." Reimbursement for flights booked on other airlines is limited to "the same cabin of service or lower" regardless of the availability of these seats.[29]

44.   Delta's definition of "reasonable costs" expressly does not include "prepaid expenses, including but not limited to hotel reservations at the customer's destination, vacation experiences, lost wages, concerts or other tickets."[30] This policy leaves Delta's customers with hundreds or thousands of dollars of nonrefundable expenses during what the Transportation

---

[27] Chris Isidore, Isabel Rosales, and Amanda Musa, *Delta is still melting down. It could last all week*, CNN (July 24, 2024), https://www.cnn.com/2024/07/23/business/delta-flight-cancellations/index.html (accessed Aug. 4, 2024).

[28] Susan Tompor, *Delta customers lost time, money. How to file claims, complaints*, USA TODAY (July 26, 2024), https://www.usatoday.com/story/travel/columnist/2024/07/26/how-delta-airlines-passengers-can-file-claims/74555651007/ (accessed Aug. 4, 2024).

[29] Staff Writer, *What Delta is doing to make things right for customers impacted by CrowdStrike disruption*, DELTA NEWS HUB (July 26, 2024), https://news.delta.com/what-delta-doing-make-things-right-customers-impacted-crowdstrike-disruption (accessed Aug. 4, 2024).

[30] DELTA NEWS HUB, *supra*.

Security Administration projected to be the busiest travel season in history,[31] and CNN stated was Delta's "busiest travel period of the summer."[32] Many of those lost experiences, such as missed weddings, concerts, or tightly-scheduled vacations, cannot be rescheduled.[33]

45.   "Reasonable costs" also do not cover the hours customers spent waiting for eventually canceled flights, making alternative travel plans, on the phone with Delta customer service, recovering luggage, or gathering and submitting the documentation needed to receive what reimbursement Delta is offering.[34]

D.   CrowdStrike Foresaw the Outage and Its Impact.

46.   CrowdStrike told its investors (and therefore likely told its customers) that its technology was validated, tested, and certified. However, CrowdStrike had instituted deficient controls for testing updates to Falcon before rolling the updates out to customers. CrowdStrike's inadequate testing created a substantial risk that an update to Falcon could cause major outages for a significant number of CrowdStrike's customers.

47.   CrowdStrike executives were aware of the difficulty of an airline trying to manually reset numerous devices on a large business's network. In a conference call with investors and investment analysts on November 28, 2023, CrowdStrike's CEO Greg Kurtz stated that

---

[31] Teodora Mitov, *TSA projects busiest travel season in history this summer*, NEWSNATION (June 12, 2024), https://www.newsnationnow.com/travel/tsa-summer-travel-season/, (accessed Aug. 4, 2024).

[32] Isidore et al., *supra*.

[33] *See* Samantha Iacia, *When Is Wedding Season? Here Are the Most Popular Wedding Months*, THE KNOT (Mar. 19, 2024), https://www.theknot.com/content/is-there-an-off-season-for-weddings, (accessed Aug. 4, 2024) (25% of couples were married between June and August 2023); Lester Fabian Brathwaite, ENTERTAINMENT WEEKLY (July 19, 2024), *Your guide to 2024's biggest music tours*, (accessed Aug. 4, 2024).

[34] Tompor, *supra*.

CrowdStrike has "many airlines that use our technology." He added, "[t]hey don't want to send out an IT person to go fix a kiosk that has a Microsoft blue screen." His solution was that they could pay CrowdStrike to use Falcon for IT.[35] Earlier in those remarks he expressed gratitude for customers who trusted CrowdStrike "as their cyber security platform *consolidator* for the AI era[.]" (emphasis added). He stated, "[f]rom hygiene to patching, Falcon for IT lets customers consolidate multiple use cases and replace legacy products with our single agent architecture."[36] But such consolidation and "single agent architecture" as CrowdStrike advocated meant that if its single agent erred, the architecture could disrupt an entire enterprise network, as CrowdStrike executives reasonably must have known.

48.   CrowdStrike executives knew or must have known from personal and company experience about the difficulties that a flawed network update could cause. CrowdStrike's current CEO George Kurtz served as a customer-facing Field Chief Technology Officer at McAfee from 2009 to 2011. In 2010, McAfee released a flawed security software update that mistakenly misidentified a critical Windows file as a virus. In an "eerily similar" incident, McAfee's error crashed millions of computers and got them stuck in reboot loops. As in the CrowdStrike Outage, the only fix for McAfee's error was manual intervention, and the problem created chaos for numerous businesses and computer users.[37]

49.   More recently, in April [2024], CrowdStrike pushed a software update to customers running on the Linux operating system that also crashed computers. That outage took CrowdStrike

---

[35] *CrowdStrike Holdings, Inc. (CRWD) Q3 2024 Earnings Call Transcript, supra.*

[36] *Id.*

[37] Adrian Volenik, *CrowdStrike CEO Was Working For McAfee in 2010 When There Was A Global Tech Outage Too*, YAHOO!FINANCE, (July 25, 2024), https://finance.yahoo.com/news/crowdstrike-ceo-involved-another-global-200015346.html (accessed August 1, 2024).

nearly five days to resolve. CrowdStrike promised those customers that it would improve its testing process going forward.[38]

50.   Accordingly, CrowdStrike knew its Falcon system concentrated security efforts into a "single agent architecture" that expanded the chaos its software error could cause, that a software error could crash and trap millions of computers in reboot loops, that it had problems with testing updates, and that in the event of an update error, its many airline customers could have problems manually rebooting numerous individual endpoints facing the blue Windows failure screen.

E.   Reasonable Precautions Would Have Prevented or Limited the Outage and Its Impact.

51.   CrowdStrike reportedly conducts some testing of its software updates but fell short of a reasonable software provider's conduct in preparing and pushing out the defective Falson update that caused the CrowdStrike Outage. CrowdStrike admitted it had a "bug" in its testing system. The bug reportedly resided in part of the validation system that runs validation checks on new updates before their release. This failure allowed the software update to be pushed out despite containing "problematic content data."[39]

52.   CrowdStrike reportedly assumed its system would work because it had been used in a March [2024] deployment.[40] But given the worldwide deployment and the potential for mischief, such an assumption about CrowdStrike's systems proved unwise and unwarranted.

---

[38] Adam Satariano, Paul Mozur, Kate Conger and Sheera Frenkel, *Chaos and Confusion: Tech Outage Causes Disruptions Worldwide*, NEW YORK TIMES (July 19, 2024), https://www.nytimes.com/2024/07/19/business/microsoft-outage-cause-azure-crowdstrike.html (accessed July 24, 2024).

[39] Fung, *supra*; Vipers and Rundle, *supra*.

[40] Warren, *supra*.

Former senior White House National Security Council director Steve Kelly called it "alarming when patches and updates that are intended for systems that have true operational impact are not tested and validated before going into production."[41]

53.   In addition to monitoring and testing its testing system, reasonable efforts to test the update and stage its distribution would have avoided or considerably limited the CrowdStrike Outage. For example, the update should have been sent to a single test computer or network of Windows computers in a quarantined system and that system should have been tried and tested with the update.[42]

54.   Similarly, CrowdStrike should have pushed out its update sequentially so it could better observe the update's effects before sending it out to the next network. Such a staged or sequential issuance would at least have limited the global effects of the update and its outage. In a staggered deployment strategy, the company initially releases updates to a small group of computers, and then availability is slowly expanded once it becomes clear the update has not caused major problems.

55.   Since the CrowdStrike Outage, CrowdStrike has promised to improve its testing to prevent similar outages. As summarized in online technology magazine THE VERGE,

> To prevent this from happening again, CrowdStrike is promising to improve its Rapid Response Content testing by using local developer testing, content update and rollback testing, alongside stress testing, fuzzing, and fault injection. CrowdStrike will also

---

[41] Joseph Menn and Aaron Gregg, *CrowdStrike Blames Global IT Outage on Bug in Checking Updates,* THE WASHINGTON POST (July 24, 2024), https://www.washingtonpost.com/business/2024/07/24/crowdstrike-microsoft-crash-bug-report/ (accessed July 31, 2024).

[42] Vipers and Rundle, *supra* (quoting former McAfee executive); Menn and Gregg, *supra* (some security experts said they were appalled to learn "that CrowdStrike had not first deployed the update to a full-fledged computer running Windows and then rolled it out gradually, so that any mistake would have been detected before it disabled computers around the world.").

perform stability testing and content interface testing on Rapid Response Content.[43]

56.   Since the Outage, CrowdStrike has stated it would improve monitoring of its system and sensor performance and would help guide a "phased rollout." CrowdStrike has also stated it will in the future give customers more control over when Rapid Response Content updates are deployed so hazardous updates do not necessarily hit all of everyone's computers when workers and IT departments are off duty (e.g, around midnight).[44]   These concessions show that CrowdStrike had control over the update and that different procedures were feasible before the CrowdStrike Outage, and would have avoided or limited the extent of the Outage.

57.   On August 10, 2024, CrowdStrike's president accepted the Pwnie [sic] computer award for the "most epic fail." He stated he was there "[b]cause we got this horribly wrong, we've said this a number of times, and it's super important to own it when you do things well, it's super important to own it when you do things horribly wrong."[45]

V.   CLASS ALLEGATIONS

58.   Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of others similarly situated pursuant to Rule 23(b)(3) and 23(c)(4) of the Federal Rules of Civil Procedure.

---

[43] Warren, *supra*.

[44] Andrew Cunningham, *CrowdStrike Blames Testing Bugs for Security Update that Took Down 8.5 M Windows PCs*, ARSTECHNICA, (July 24, 2024), https://arstechnica.com/information-technology/2024/07/crowdstrike-blames-testing-bugs-for-security-update-that-took-down-8-5m-windows-pcs/ (accessed July 27, 2024); Menn and Gregg, *supra* (CrowdStrike said it would improve testing, stagger distribution, and give customers control over whether small updates are installed immediately).

[45] Anthony Ha, *CrowdStrike Accepts Award for 'Most Epic Fail'' After Global IT Outage,* TECHCRUNCH (Aug. 11, 2024), https://techcrunch.com/2024/08/11/crowdstrike-accepts-award-for-most-epic-fail-after-global-it-outage/ (accessed August 16, 2024).

59.   The Nationwide Class that Plaintiffs seek to represent is defined as follows:

> All customers of Delta Airlines who are citizens or legal residents of the United States who (a) had flight reservations with Delta Airlines as of 11:59 p.m. on July 18, 2024, and (b) whose flights were delayed or canceled between July 19, 2024, and July 26, 2024 (the "Class Period"), and (c) were unable to reach their destination (or return to their starting point) as scheduled and (d) incurred losses due to cancellation fees, hotel or food expenses, substitute airline flights or other transportation costs, or concerts or other events they were unable to attend.

60.   Alternately, Plaintiffs seek to represent the Iowa statewide class, defined as follows:

> All customers of Delta Airlines who are citizens or legal residents of Iowa who (a) had flight reservations with Delta Airlines as of 11:59 p.m. on July 18, 2024, and (b) whose flights were delayed or canceled between July 19, 2024, and July 26, 2024 (the "Class Period"), and (c) were unable to reach their destination (or return to their starting point) as scheduled and (d) incurred losses due to cancellation fees, hotel or food expenses, substitute airline flights or other transportation costs, or concerts or other events they were unable to attend.

61.   Excluded from the Class are the following individuals and/or entities: CrowdStrike and its parents, subsidiaries, affiliates, officers, and directors, and any entity in which CrowdStrike has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state, or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, councils and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

62.   Plaintiffs reserve the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

63.   <u>Numerosity</u>, Fed. R. Civ. P. 23(a)(1): Class Members are so numerous that joinder of all members is impracticable. Delta canceled thousands of flights across the United States

18

because of the CrowdStrike Outage, many of which had dozens or hundreds of passengers booked to fill their seats. Accordingly, thousands of Class Members' flights were canceled or postponed. Their identities can be readily determined from Delta's records and the Class Members' own records of their travel arrangements and cancellations.

64.   Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of fact common to the Class exist and predominate over any questions affecting only individual Class Members. These common questions include:

a)   What failures by CrowdStrike caused the CrowdStrike Outage;

b)   Whether CrowdStrike had information about other similar computer outage events;

c)   Whether CrowdStrike failed to properly review, assess, and manage the risks posed by its simultaneous update to thousands of computer networks and the networks' endpoints;

d)   Whether CrowdStrike committed negligent acts in preparing and pushing out its Falcon software update;

e)   What testing CrowdStrike conducted or failed to conduct before pushing out the Falcon software update;

f)   What facts did CrowdStrike have in its possession about Delta's use of CrowdStrike Falcon software;

g)   What facts did CrowdStrike have in its possession about Delta's agreements with and commitments to Class Members for the Class Members' travel, generally and for the period in which air travel was affected by the CrowdStrike Outage;

h)   Whether Plaintiffs and Class Members are entitled to actual

damages as a result of CrowdStrike's wrongful conduct.

65.   Typicality, Fed R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of those of other

Class Members because all had Delta air flights canceled or postponed and sustained losses for

hotel bills, substitute air flights or other transportation alternatives, and/or losses from concerts or

other events they were unable to attend because of the CrowdStrike Outage.

66.   Predominance: CrowdStrike engaged in a common course of conduct toward

Plaintiffs and other Class Members, in that CrowdStrike's improperly executed software update

caused their flights to be canceled, imposing unwanted costs on the Class Members. The common

issues arising from CrowdStrike's conduct affecting Class Members set out above predominate

over any individualized issues. Adjudication of these issues in a single action has important and

desirable advantages of judicial economy. CrowdStrike's procedures and uniform update actions

apply to and affect Class Members uniformly and Plaintiffs' challenge to those actions hinges on

CrowdStrike's conduct with respect to the Class as a whole, not on facts or law applicable only to

Plaintiffs.

67.   Adequacy of Representation, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and

adequately represent and protect the interests of the Class Members in that Plaintiffs have no

disabling conflicts of interest that would be antagonistic to those of the other Members of the Class.

Plaintiffs seek no relief that is adverse to the other Class Members and the infringement of rights

and the damages Plaintiffs sustained are typical of those of other Class Members. Plaintiffs have

retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute

this action vigorously.

68.   Superiority, Fed. R. Civ. P. 23(b)(3): Class-wide litigation is an appropriate method for fairly and efficiently adjudicating the claims involved in this case. Class treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations like CrowdStrike. Further, even for those Class Members who could afford to litigate such a claim, such an approach would be economically impractical for the Class Members and impose a burden on the courts.

69.   The nature of this action and the nature of laws available to Plaintiffs and other Class Members make using class action procedure especially efficient and appropriate for remedying the wrongs imposed on them because CrowdStrike would necessarily gain an unconscionable advantage since it could exploit and overwhelm the limited resources of each individual Class Member with the superior financial and legal resources available to a public corporation with a $77.4 billion market valuation; the costs of individual suits would unreasonably consume the amounts that individual plaintiffs could recover; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the causes of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

70.   Litigating the claims brought herein by a class action is manageable. CrowdStrike's uniform conduct, including its software and update testing and its methods for pushing out updates

to numerous customers' computer networks, the consistent provisions of relevant legal doctrine, and the ascertainable identities of Class Members demonstrates that prosecuting this lawsuit as a class action would entail no significant manageability problems.

71.   Adequate notice can be given to Class Members directly by using information maintained in Delta Airlines' records.

72.   CrowdStrike has acted or failed to act on grounds generally applicable to the Class, so class certification and resulting relief are appropriate on a class-wide basis.

73.   Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein.   Such particular issues include, but are not limited to:

      a)   What failures by CrowdStrike caused the CrowdStrike Outage;

      b)   Whether CrowdStrike had information about other similar computer outage events;

      c)   Whether CrowdStrike failed to properly review, assess, and manage the risks posed by its simultaneous update to thousands of computer networks and the networks' endpoints;

      d)   Whether CrowdStrike committed negligent acts in preparing and pushing out its Falcon software update;

      e)   What testing CrowdStrike conducted or failed to conduct before pushing out the Falcon software update;

      f)   What facts did CrowdStrike have in its possession about Delta's use of CrowdStrike Falcon software;

g)   What facts did CrowdStrike have in its possession about Delta's

agreements with and commitments to Class Members for the Class

Members' travel, generally and for the period in which air travel was

affected by the CrowdStrike Outage;

VI.   CLAIMS FOR RELIEF

A.   Negligent Design and Implementation of the Falcon Update
(Plaintiffs and the Nationwide or Statewide Class, Against CrowdStrike)

74.   Plaintiffs incorporate by reference the allegations contained in the paragraphs

above as if set forth fully herein.

75.   CrowdStrike owed Plaintiffs and other Class Members a duty to act with reasonable

care to maintain Delta Airlines' computer network and endpoints in a secure and reliable system

that would function properly and maintain customers' flight schedules. Delta used its computer

networks, computers, and computer terminals to keep its flights traveling on schedule.

76.   CrowdStrike also owed Plaintiffs and other Class Members a duty not to cause harm

to Plaintiffs and Class Members because they were foreseeable and probable victims of

substandard cybersecurity updates like the update that caused the CrowdStrike Outage. Their harm

was foreseeable because if Delta's computer network and endpoints failed, then its systems for

finding crew, maintaining airplanes, and commencing air flights one after another would sustain a

meltdown like the CrowdStrike Outage caused.

77.   CrowdStrike knew or should have known of the vulnerabilities of their

cybersecurity system, especially since they designed and pursued a single architecture system and

encouraged customers to replace all their legacy cybersecurity systems with CrowdStrike's Falcon.

CrowdStrike also knew that it embedded its Falcon software deeply with the Windows operating

system in such a way that errors in the Falcon software could readily spread to the rest of the

computer's operating system and cause the computer's operating system to crash. CrowdStrike

also knew that Delta and many of CrowdStrike's customers were commercial passenger airlines

that would have difficulty going "to fix a kiosk that has a Microsoft blue screen." CrowdStrike

also knew through its own previous experience and that of its CEO that a flawed security update

could crash millions of computers and get them stuck in reboot loops, which could take days to

resolve.

78.   By pressing a single architecture cybersecurity system, CrowdStrike undertook to

act with reasonable care and awareness of the potential widespread chaos that an update error

would likely cause for its customers and their customers.

79.   CrowdStrike breached its duties to Plaintiffs and other Class Members in several

ways concerning the design and implementation of its Falcon cybersecurity software and updates

to the Falcon endpoint software, including by:

a)   Designing a system that would make an entire enterprise

dependent on the same system that replaced customers'

legacy systems and eliminating alternative and redundant

systems;

b)   Designing a system where programming or update errors

could easily spread from Falcon to the computer's operating

system, more easily causing crashes and reboot loops; and,

c)   Designing a system with apparently simultaneous, or nearly

simultaneous, distribution to all networks and endpoints of

all of CrowdStrike's customers, rather than a sequential or

staged distribution with an initially quarantined network and

gradual distribution to customers' networks.

80.   CrowdStrike's breach of its duty of care caused the CrowdStrike Outage that disrupted thousands of air flights for Plaintiffs and other Class Members. As a direct and proximate result of CrowdStrike's conduct, Plaintiffs and Class Members have suffered damages discussed in this complaint, including missed flights and connections, replacement flights and other alternative transportation costs, hotel bills, meals away from home at additional costs, and lost value of concert tickets and other events they missed because of their missed and canceled flights.

B.   Negligent Failure to Test
 (Plaintiffs and the Nationwide or Statewide Class, Against CrowdStrike)

81.   Plaintiffs incorporate by reference the allegations contained in the paragraphs above as if set forth fully herein.

82.   CrowdStrike owed Plaintiffs and other Class Members a duty to act with reasonable care to maintain Delta Airlines' computer network and endpoints in a secure and reliable system that would function properly and maintain customers' flight schedules. Delta used its computer networks, computers, and computer terminals to keep its flights traveling on schedule.

83.   CrowdStrike also owed Plaintiffs and other Class Members a duty not to cause harm to Plaintiffs and Class Members because they were foreseeable and probable victims of substandard cybersecurity and computer operating system updates like the update that caused the CrowdStrike Outage because if Delta's computer network and endpoints failed, then its systems for finding crew, safely maintaining airplanes, and commencing air flights one after another would sustain a meltdown like the CrowdStrike Outage caused.

84.   CrowdStrike knew or should have known of the vulnerabilities of their cybersecurity system, especially since they designed and pursued a single architecture system and

encouraged customers to replace all their legacy cybersecurity systems with CrowdStrike's Falcon. CrowdStrike also knew that it embedded its Falcon software deeply with the Windows operating system, in such a way that errors in the Falcon software could readily spread to the rest of the computer's operating system and cause the computer's operating system to crash. CrowdStrike also knew that Delta and many of CrowdStrike's customers were commercial passenger airlines that would have difficulty going "to fix a kiosk that has a Microsoft blue screen." CrowdStrike also knew through its own previous experience and that of its CEO that a flawed security update could crash millions of computers and get them stuck in reboot loops, which could take days to resolve.

85.   CrowdStrike has admitted it had a "bug" in its testing system. The bug reportedly resided in part of the validation system that runs validation checks on new updates before their release. This failure allowed the software update to be pushed out despite containing "problematic content data."[46]

86.   CrowdStrike breached its duty of care to Plaintiffs and other Class Members with respect to testing in multiple ways, including the following:

a)   By assuming CrowdStrike's update system would work because it had worked before;

b)   By failing to test and validate the update system again before pushing out a system-wide update to so many customers, networks, and endpoints;

---

[46] Fung, *supra*; Vipers and Rundle, *supra*.

c)   By failing to test the update's implementation with a "canary

system" of a single quarantined computer or computer

network;

87.   Improved alternative update testing was practical and feasible, as suggested by CrowdStrike's statements of what it would do differently to avoid future incidents like the CrowdStrike Outage.

88.   CrowdStrike's breach of its duty of care caused the CrowdStrike Outage that disrupted thousands of air flights for Plaintiffs and other Class Members. As a direct and proximate result of CrowdStrike's conduct, Plaintiffs and Class Members have suffered damages discussed in this complaint, including missed flights and connections, replacement flights and other alternative transportation costs, hotel bills, meals away from home at additional costs, and lost value of concert tickets and other events they missed because of their missed and canceled flights.

C.   Negligent Failure to Warn
(Plaintiffs and the Nationwide or Statewide Class, Against CrowdStrike)

89.   Plaintiffs incorporate by reference the allegations contained in the paragraphs above as if set forth fully herein.

90.   CrowdStrike owed a duty to warn Delta Airlines, Plaintiffs, and other Class Members of the danger that it would cause Delta to experience widespread computer outages due to CrowdStrike's design of its software, the way it interacts with Windows operating systems, and CrowdStrike's casual methods for updating its software, for the following reasons.

91.   CrowdStrike undertook to provide updating of cybersecurity software deeply embedded in the operating systems of Delta's many computer systems. CrowdStrike controlled the updating system for its Falcon software and could push its software updates directly from its own facilities to Delta's computers and other network endpoints. CrowdStrike knew its cybersecurity

software and updating computer operating systems were necessary for protecting air passengers from malicious computer viruses and defective computer systems that impaired air flights.

92.   CrowdStrike failed to exercise reasonable care in performing its services of designing and implementing its Falcon software and its updates of the software, as previously alleged.

93.   Delta and its passengers, Plaintiffs and other Class Members, relied on CrowdStrike's performance of its ongoing services to keep Delta's airplanes flying as scheduled.

94.   Delta's performance in its implementation of its subscription software and updates to that software, which caused the CrowdStrike Outage, increased the risk to Delta and to Plaintiffs and the other Class Members that Delta's airplanes would fail to fly and transport passengers as scheduled.

95.   CrowdStrike also owed Delta, Plaintiffs, and other Class Members a duty to warn because of CrowdStrike's superior knowledge about its software system, its updating process, and the hazards they posed for air travel.

96.   CrowdStrike knew its Falcon software system and its method of updating that system posed a substantial risk of harm to Delta and Delta's customers.

97.   Delta and its customers could have been located through Delta's records. Delta collects air travelers' names and other information when they book their air tickets.[47] A warning could have been provided to Delta's customers using that information from booking. A 2005

---

[47] *See* Eric Jordan and Louis Cheslaw, *Can You Change the Name on an Airline Ticket?* CONDE NAST TRAVELER (July 26, 2023), https://www.cntraveler.com/stories/2014-11-07/whats-in-a-name-the-truth-about-name-changes-on-airline-tickets (accessed August 5, 2024) ("TSA rules say the name on the boarding pass must exactly match the passenger's government-issued ID presented at the security checkpoint.").

article stated software vendors "possess technology to track antivirus software and to warn users if their protection is not installed or properly updated."[48]

98.   At the very least, CrowdStrike could have provided a warning to Delta and Delta's staff of these hazards. For example, warnings could have systematically popped up on Delta employees' computer screens that an update had been installed, that future updates would be installed, and that future updates might cause Delta's computers to crash and require manual rebooting by Delta's IT department.

99.   The risk of harm to Delta and its customers was sufficiently great to justify the burden of providing a warning.

100.   CrowdStrike failed to provide any warning to Plaintiffs or the other Class Members of the risks of its Falcon software system and its methods of updating that software. CrowdStrike thereby breached its duty to warn.

101.   If Plaintiffs and the other Class Members had received adequate warnings of the risk of the CrowdStrike Outage, then they could have avoided the risk of traveling then, could have booked refundable tickets, or made contingency plans for cancellation of their flights. Accordingly, CrowdStrike's breach of its duty to warn directly and proximately caused harm and damages to Plaintiffs and other Class Members.

D.   Interference With Plaintiffs' Contract With Delta Airlines
(Plaintiffs and the Nationwide or Statewide Class, Against CrowdStrike)

102.   Plaintiffs incorporate by reference the allegations contained in the paragraphs above as if set forth fully herein.

---

[48] Rustad and Hoenig, *The Tort of Negligent Enablement of Cybercrime*, 20 BERKELEY TECH. L.J. 1553, 1567 (2005).

103.   Plaintiffs and other Class Members had contracts with Delta Airlines for Delta to transport the passengers on commercial airline flights from their starting point to their destination with specified starting and arrival times. CrowdStrike's CEO was aware of these agreements, as shown by his comments to investors and analysts that "many airlines use our technology." He demonstrated awareness of how commercial flights operate at airports by his comment that airlines "don't want to send out an IT person to go fix a kiosk that has a Microsoft blue screen," referring to check-in kiosks at public airports.

104.   CrowdStrike also knew, from both its corporate experience and its CEO's prior experience at McAfee, that an error in a security update could crash millions of computer endpoints and trap them in reboot doom loops, particularly given its single-system architecture installed deeply into the Windows operating software. Therefore, CrowdStrike knew that a defective update of its software would crash numerous customer airline computer systems, including those of Delta Airlines.

105.   CrowdStrike's actions in causing the CrowdStrike Outage knowingly and willfully interfered with the contracts between Plaintiffs and Delta Airlines, and between Delta Airlines and the other Class Members.

106.   CrowdStrike's actions in causing the CrowdStrike Outage and Delta's meltdown of its computer systems directly caused Delta to cancel thousands of flights for which they had contracts with Plaintiffs and other Class Members. As described herein, those cancellations directly harmed Plaintiffs and the other Class Members.

VII.   REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of other Members of the Classes, respectfully request that the Court enter judgment in their favor and against CrowdStrike, as follows:

A.   Certifying the proposed Nationwide and State Classes, including appointment of Plaintiffs' counsel as Class counsel;

B.   Awarding damages for Plaintiffs and the other Class Members for their unreimbursed losses for missed flights and connections, replacement flights and other alternative transportation costs, hotel bills, meals away from home at additional costs, and lost value of concert tickets and other events they missed because of their missed and canceled flights;

C.   Ordering CrowdStrike to pay pre- and post-judgment interest on any damages awarded;

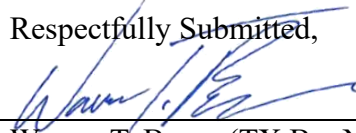D.   Awarding costs and attorneys' fees; and,

E.   Granting such other or further relief as may be appropriate.

VII.   DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a jury trial for all claims so triable.

31

Dated: August 19, 2024

Respectfully Submitted,

Warren T. Burns (TX Bar No. 24053119)
Kyle Oxford (TX Bar No. 24095806)
BURNS CHAREST LLP
900 Jackson Street, Suite 500
Dallas, Texas 75202
Telephone: (469) 904-4550
wburns@burnscharest.com
koxford@burnscharest.com

Korey A. Nelson *(to be admitted pro hac vice)*
BURNS CHAREST LLP
365 Canal Street, Suite 1170
New Orleans, Louisiana 70130
Telephone: (504) 799-2845
knelson@burnscharest.com

Robert K. Shelquist *(to be admitted pro hac vice)*
Rebecca A. Peterson *(to be admitted pro hac vice)*
Craig S. Davis *(to be admitted pro hac vice)*
LOCKRIDGE GRINDAL NAUEN PLLP
100 Washington Avenue South, Suite 2200
Minneapolis, Minnesota 55401
Telephone: (612) 339-6900
rkshelquist@locklaw.com
rapeterson@locklaw.com
csdavis@locklaw.com

Charles J. LaDuca *(to be admitted pro hac vice)*
Brendan Thompson *(to be admitted pro hac vice)*
CUNEO GILBERT & LADUCA, LLP
4725 Wisconsin Avenue NW
Washington, D.C. 20016
Telephone: (202) 789-3960
charlesl@cuneolaw.com
brendan@cuneolaw.com

J. Barton Goplerud *(to be admitted pro hac vice)*
SHINDLER, ANDERSON, GOPLERUD & WEESE, P.C.
5015 Grand Ridge Drive, Suite 100
West Des Moines, Iowa 50265
Telephone: (515) 223-4567
goplerud@sagwlaw.com

Attorneys for Plaintiffs